REMARKS

Reconsideration of the above-identified patent application in view of the amendments above and the remarks following is respectfully requested.

Claims 1-42 are in this case. Claims 1-6, 9-11, 14, 17-21, 24, 25, 28-31, 33, 34, 36, 39, 41 and 42 have been rejected under § 102(b). Claims 7, 8, 12, 13, 15, 16, 22, 23, 26, 27, 32, 35, 37, 38 and 40 have been rejected under § 103(a). Dependent claims 9, 12, 13, 22, 23 and 40 have been canceled. Independent claims 1, 17 and 28 and dependent claims 2, 3, 6-8, 10, 11, 14-16, 36-39, 41 and 42 have been amended. New independent claims 47-54 and new dependent claims 43-46 have been added.

The claims before the Examiner are directed toward a device and system for digital rights management and a method of their use. The system includes the device and a server. Encrypted digital data stored at the server. The device includes an integrated circuit that includes a processor and a player. The device also includes a flash memory. The processor requests the server to transmit the encrypted digital data to the device, and decrypts the data. The encrypted data are stored in the flash memory. The player transforms the decrypted data to analog signals.

§ 102(b) Rejections – Davis '879

The Examiner has rejected claims 1-6, 9-11, 14, 17-21, 24, 25, 28-31, 33, 34, 36, 39, 41 and 42 under § 102(b) as being anticipated by Davis, US Patent No. 5,825,879 (henceforth, "Davis '879"). The Examiner's rejection is respectfully traversed.

Claim 9 now has been canceled, thereby rendering moot the Examiner's rejection of this claim.

Independent claims 1, 17 and 28 have been amended as discussed below in the context of the § 103(a) rejections, and now are in condition for allowance. It follows that claims 2-6, 10, 11, 14, 17-21, 24, 25, 28-31, 33, 34, 36, 39, 41 and 42, that depend therefrom, also are allowable.

§ 103(a) Rejections – Davis '879

The Examiner has rejected claims 12, 13, 15, 16, 22, 23, 26, 27, 32, 35, 38 and 40 under § 103(a) as being unpatentable over Davis '879. The Examiner's rejection is respectfully traversed.

Davis '879 teaches a secure video content processor (SVCP) **302** that receives encrypted video content **308**, decrypts and decompresses encrypted video content **308** using decryption and decompression circuitry **312**, generates corresponding video frames using a graphics processor **316**, and uses a D/A converter **326** to convert the video frames to analog signals for display on a display device **332**. As needed, video frames are encrypted using a frame data encryptor **320**, stored in a frame buffer **300** outside of SVCP **302**, recovered from frame buffer **302** and decrypted using a frame data decryptor **324**.

Independent claim 1 as filed recites an integrated circuit that comprises a processor with functionality similar to that of decryption and decompression circuitry **312** and frame data decryptor **324** and a player with functionality similar to that of D/A converter **326**. Claim 13 adds to independent claim 1 the limitation that a device that comprises the integrated circuit of claim 1 also comprises a flash memory for storing the encrypted digital data. Independent claim 17 as filed recites a system that comprises a user platform that includes the integrated circuit of claim 1. Claim 23 adds to independent claim 17 the limitation that the user platform also includes a flash memory for storing the encrypted digital data. The Examiner has rejected claims 13

and 23 on the grounds that storing encrypted digital data in a non-volatile memory such as a flash memory is well-known in the art, so that it would be obvious to substitute a flash memory for frame buffer **300**, thereby obtaining the device of the present invention as recited in claim 13 or the system of the present invention as recited in claim 23. What the Examiner has overlooked is that the entire context of Davis '879 is the display of video data, so that one ordinarily skilled in the art would modify the invention of Davis '879 only in that context. In particular, one ordinarily skilled in the art would not substitute a flash memory for frame buffer **300** because a flash memory would be too slow to serve as a frame buffer for video frames. Consider, for example, a video frame intended for display on a display device **332** with a resolution of 1024 x 1280 pixels and that supports 64K colors (two eight-bit bytes per pixels), at a refresh rate of 30 frames per second. Each frame includes 1024 x 1280 x 2 = 2,621,440 bytes. The rate at which data must be written to and read from frame buffer **300** therefore is approximately 78.6 Mbytes per second. No currently available flash disk can be written and then read that fast. The top speed for merely writing to the fastest currently available NAND flash memory is only on the order of a few Mbytes per second. The NAND flash memories that were available on the priority date of the above-referenced patent application were even slower. Writing to a NOR flash memory is slower than writing to a NAND flash memory. On the priority date of the above-referenced patent application, flash memories were simply too slow to be substituted for frame buffer **300**.

Therefore, independent claim 1 has been amended to recite its integrated circuit in the context of a device for digital rights management, as recited in claim 9, and has been further amended to include the limitations of claims 12 and 13. Similarly, independent claim 17 has been amended to include the limitations of claims

22 and 23, and independent claim 28 has been amended to include the limitations of claim 40 (the additional step of storing the encrypted data in a non-volatile memory) and the further limitation that the non-volatile memory is a flash memory. Support for these amendments is found in claims 13 and 23 as filed. Correspondingly, claims 9, 12, 13, 22, 23 and 40 have been canceled, claims 10 and 11 have been amended to depend directly from claim 1, and claims 2-8 and 14-16 have been amended to recite a "device" instead of an "integrated circuit".

Amended independent claims 1, 17 and 28 now feature language which makes it absolutely clear that the present invention stores the encrypted digital data in a flash memory. Applicant believes that the amendment of the claims completely overcomes the Examiner's rejections on § 103(a) grounds.

With independent claims 1, 17 and 28 allowable in their present form, it follows that claims 15, 16, 26, 27, 32, 35 and 38, that depend therefrom, also are allowable.

§ 103(a) Rejections – Davis '879 in view of Dlugosch '146

The Examiner has rejected claims 7 and 8 under § 103(a) as being unpatentable over Davis '879 in view of Dlugosch, US Patent No. 6,789,146. The Examiner's rejection is respectfully traversed.

It is demonstrated above that independent claim 1 is allowable in its present form. It follows that claims 7 and 8, that depend therefrom, also are allowable.

Other Amendments to the Claims

The preambles of independent claims 17 and 28 have been simplified to recite a system for, and a method of, digital rights management, as stated in the title of the above-identified patent application as well as on page 10 lines 9-10 of the

specification. In accordance with this amendment to the preamble of claim 28, the step of storing encrypted digital data at a server has been added to the body of the claim. This additional step is supported in the specification in Figure 1 as described on page 2 lines 6-8.

New Claims

New dependent claims 43-46 have been added to recite the limitations of claims 4 and 5 in the context of claims 17 and 28.

In addition, new independent claims 47-54 have been added.

As noted above, the context of Davis '879 is specifically video data. Although it could be argued that Davis '879 anticipates claim 4 as filed because video files usually include audio soundtracks, Davis '879 certainly does not anticipate an integrated circuit, a system or a method that is limited to only digital audio data. Furthermore, because one ordinarily skilled in the art would not contemplate any utility to the invention of Davis '879 outside the context of video data, this limitation is not even obvious from Davis '879. New claim 47 is independent claim 1 as filed and including this limitation. New claims 48 and 49 are independent claims 17 and 28 as filed, with their preambles simplified as described above, and also including this limitation. Support for this limitation is found in the specification on page 3 lines 4-8:

> For example, if the downloaded data are audio data, player **20** could be an MP3 player. Player **20** then transforms the decrypted digital audio data to analog signals, optionally amplifies the analog signals, and sends the analog signals to a speaker **24** that transforms the audio signals into audible sound.

combined with page 11 line 21 through page 12 line 2:

> Player **34** differs from player **20** in that unlike player **20**, player **34** does no digital processing of its own. Player **34** essentially is just a digital-to-analog converter that transforms the decrypted digital data to analog signals that are transformed to user-perceptible sensations by display mechanism **24**. For example, if the digital data are audio data,

then display mechanism **24** is a speaker that transforms the analog signals to audible sound.

Contrary to the Examiner's grounds for rejecting claim 41 as filed, Davis '879 does not teach resetting SVCP **302** when an attempt to tamper with SVCP **302** is detected. Similarly, Davis '879 does not teach the provision of sensors to detect such tampering so that SVCP **302** can be reset. Davis '879 teaches only two methods of securing SVCP **302** against tampering: making it structurally difficult to tamper with SVCP **302** (column 4 lines 34-35: "This hardware barrier **222** may merely resist opening without significant force"; column 4 lines 43-46: "the hardware barrier **222** may exist because the various components are integrated on a single chip making it physically difficult to tap into the microscopic wires on the chip"); and arranging SVCP **302** so that tampering with SVCP **302** destroys SVCP **302** (column 4 lines 35-36: "the barrier may destroy the interior circuitry if the outer case is opened").

Therefore, new claims 50-52 have been added. New claim 50 is independent claim 1 as filed and also including the limitations that the decryption of the encrypted digital data is effected using one or more keys and that the integrated circuit includes one or more sensors for detecting an attempt to hack the key(s). New claim 51 is independent claim 17 as filed, with its preamble simplified as described above, and also including the limitations that the decryption of the encrypted digital data is effected using one or more keys and that the integrated circuit includes one or more sensors for detecting an attempt to hack the key(s). Support for these limitations is found in the specification in sensors **42** of Figure 2, as described on page 12 lines 16-18:

> Detection by one of sensors **42** of an attempt to tamper with ASIC **30** triggers a reset of ASIC **30** to prevent a hacker from reading the cryptographic keys off of bus **58**.

in the context of page 13 lines 16-19:

> Processor **32** then uses flash controller **40** to retrieve the encrypted digital data from flash memory **22** and then uses coprocessor **36** and the appropriate decryption keys from EEPROM **56** to decrypt the encrypted digital data.

New claim 52 is claim 41 as filed, rewritten in independent form, and with its preamble simplified as described above.

In the invention of Davis '879, the encrypted digital data that are received by SVCP **302** are not the same as the encrypted digital data that are stored in frame buffer **300** by SVCP **302**. Encrypted video content **308** is decompressed by decompression circuitry **312** and is converted by graphics processor **316** into video frames. It is encrypted versions of these video frames, and not the received encrypted video content **308**, that is stored in frame buffer **300**. Therefore, new independent claim 53 has been added. New independent claim 53 is independent claim 28 as filed, with its preamble simplified as described above, and also including the further limitation that the processor receives the encrypted digital data and stores the received encrypted digital data in a memory separate from the integrated circuit. Support for the added limitation is found in the specification on page 13 lines 7-9:

> Processor **32** receives the requested encrypted digital data via transceiver **12** and controller **16**, and uses flash controller **40** to store the received encrypted digital data in flash memory **38**.

In rejecting claim 37, the Examiner asserted that it would be obvious to use non-volatile memory for storage "in order to save and preserve valuable data in case of power outage". However, one ordinarily skilled in the art would put such a non-volatile memory, for storing a decryption key, <u>inside</u> SVCP **302**, for two reasons. First, Davis '879 teaches placing a memory (frame buffer **300**) that is needed by his SVCP outside of his SVCP only if that memory is too large to fit inside the SVCP. Davis '879 states this explicitly in column 5 lines 12-17:

> Often, the memory requirements of the SVCP **200** exceed that which can be conveniently fabricated in a frame buffer **234** on the SVCP **200**. Thus it may be necessary to place the frame buffer outside the hardware barrier **304** surrounding the SVCP **302** as shown in FIG. 3 as secure frame buffer **300**.

Unlike a non-volatile substitute for frame buffer **300**, a non-volatile memory for storing one or more decryption keys would fit easily inside one of the SVCPs of Davis '879. Second, storing a decryption key outside of an SVCP renders the key vulnerable to hacking as the key is written or read, necessitating the extra steps of encrypting the key for writing and decrypting the key upon reading. Therefore, new independent claim 54 has been added. New independent claim 54 is claim 37 as filed, rewritten in independent form, with its preamble simplified as described above, and also including the further limitation that the nonvolatile memory in which the key(s) is/are stored is separate from the integrated circuit. Support for the additional limitation is found in the specification on page 13 lines 12-13:

> Alternatively, coprocessor **32** encrypts the decryption key(s) and uses flash controller **40** to store the encrypted decryption key(s) in flash memory **38**.

In view of the above amendments and remarks it is respectfully submitted that independent claims 1, 17, 28 and 47-54, and hence dependent claims 1-8, 10, 11, 14-16, 18-21, 24-27, 29-39 and 41-46 are in condition for allowance. Prompt notice of allowance is respectfully and earnestly solicited.

Respectfully submitted,

Mark M. Friedman
Attorney for Applicant
Registration No. 33,883

Date: March 31, 2005